UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION AT DAYTON

LIST INDUSTRIES, INC., Plaintiff, vs. DEAN SCOTT UMINA, et al., Defendants.	:	Case No. 3:18-cv-199 District Judge Thomas M. Rose Magistrate Judge Sharon L. Ovington

ORDER

I. INTRODUCTION

Plaintiff List Industries, LLC (List) brings this action for breach of the confidentiality provision of an employment contract and misappropriation in violation of Ohio's Trade Secret Act § 1333.61. The gravamen of List's Complaint is that Defendant Dean Scott Umina, a former employee, violated his Employment Agreement by unlawfully retaining one of List's hard drives after his termination and accessing it during his post-List employment with Defendant Top Tier Storage Products. List now seeks production of forensic imaging for the hard drive and two computers that allegedly were used to access the contents of the hard drive. Forensic imaging,[1] a nascent form of discovery, is requested by List for purposes of detecting pertinent activity on Defendants' devices, rather than obtaining documents.

[1] "A forensic image is an exact bit-for-bit duplications of a storage device. It does not alter anything on the original device, and is verifiable, meaning it uses hash values to confirm an exact bit-for-bit match." (Doc. #15, *PageID* #84) (citation omitted).

This case is presently before the Court upon Plaintiff's Motion to Compel (Doc. #15), Defendants' Memorandum in Opposition (Doc. #17), Plaintiff's Reply in Support (Doc. #19), and the record as a whole.

II. BACKGROUND

In August 2010, Plaintiff List purchased "all, or substantially all," of the assets of Midwest Factory Warehouse, a company owned by Defendant Umina. (Doc. #15, *PageID* #88); *see also* Doc. #17-1. As part of the Purchase and Sale Agreement, List also entered into an Employment Agreement with Defendant Umina. Under Section 7 of that Agreement, Defendant Umina agreed to refrain from "either directly or indirectly, divulge[ing], disclos[ing], or communicat[ing] to any person, firm or corporation any information relating to the business or affairs of the Company which is confidential, proprietary, or not in the public domain." (Doc. #15, *PageID* #89). Defendant Umina further agreed that "upon termination of employment, [Umina] shall return all property, materials, files and any other [List] owned information to [List]." *Id*. List alleges that Defendant Umina failed to comply with these terms of the Employment Agreement. *Id.* at 88.

A few years after the termination of his employment with List, Defendant Umina began working on the formation of Defendant Top Tier—a company that, according to List, was intended to compete with List in the storage locker industry. *Id.* at 89; (Doc. #17, *PageID* #138). List alleges that as part of a lawsuit between the parties in the Broward County, Florida Circuit Court, Defendant Umina "testified that he accessed and used at least one of List's business documents after his termination from List, and while

he was employed at Top Tier."[2] (Doc. #15, *PageID* #84). This serves as the basis for List's contention that forensic imaging of the hard drive, desktop computer, and laptop computer is necessary to obtain probative evidence connected to List's claims. *Id.* at 87-88.

The parties first discussed the request for a forensic image of the hard drive at their Rule 26(f) conference on August 30, 2018. (Doc. #17, *PageID* #146); (Doc. #19, *PageID* #264). A few days later, Defendants provided List with a protocol for imaging from their expert, Mr. Jim Swauger. (Doc. #19, *PageID* #264) (citing Kulka Dec., ¶ 4, Exhibit B). In response, List agreed to the protocol and described additional requirements for the forensic imaging as requested by List's expert, Dr. Andrew Cobb. *Id*. (citing Kulka Dec., ¶ 3, Exhibit A). Defendants' counsel subsequently informed List's counsel that "'[List's] expert can coordinate a time with [Defendants' expert] for his own inspection and imaging at a time convenient for both of them.'" *Id.* (quoting Kulka Dec., ¶ 4, Exhibit B).

On September 13, 2018, List served a Request for Inspection of the hard drive and "[a]ny electronic device used to access the information contained on the hard drive described in Plaintiff's Complaint." *Id.* (citations omitted). Defendants' expert, however, imaged the hard drive without Dr. Cobb's involvement. (Doc. #15, *PageID* #90). Shortly thereafter, on October 8, 2018, Defendants informed List that "they 'do not intend to produce forensic images of those additional devices.'" (Doc. #19, *PageID*

[2] The Florida case was dismissed for lack of personal jurisdiction. (Doc. #17, *PageID* #142).

#265) (quoting Kulka Dec., ¶ 8, Exhibit G). Soon after, Defendants denied List's request due to the vast amount of information on the hard drive. (Doc. #17, *PageID* #147). List sought informal resolution through this Court, which proved unsuccessful. *Id.*

III. STANDARD OF REVIEW

The scope of discovery under the Federal Rules of Civil Procedure is "traditionally quite broad." *Lewis v. ACB Bus. Servs, Inc.*, 135 F.3d 389, 402 (6th Cir. 1998) (citing *Mellon v. Cooper-Jarrett, Inc.*, 424 F.2d 499, 501 (6th Cir. 1970)).

> Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable.

Fed. R. Civ. P. 26(b)(1). Trial courts are granted "wide discretion in balancing the needs and rights of both plaintiff and defendant." *Scales v. J.C. Bradford Co.*, 925 F.2d 901, 906 (6th Cir. 1991).

Rule 37 provides that "[a] party seeking discovery may move for an order compelling an answer, designation, production or inspection" if a party fails to provide discovery responses. Fed. R. Civ. P. 37(a)(3)(B). First, however, that party must initially demonstrate that the information sought is relevant under Rule 26. See *Guinn v. Mount Carmel Health Sys.*, No. 2:09-cv-0226, 2010 WL 2927254, at *5 (S.D. Ohio July 23,

2010) (internal citations omitted). "When the information sought appears to be relevant, the party resisting production has the burden of establishing that the information either is not relevant or is so marginally relevant that the presumption of broad disclosure is outweighed by the potential for undue burden or harm." *Wagner v. Circle W Mastiffs*, No. 2:08-cv-431, 2013 WL 4479070, at *3 (S.D. Ohio Aug. 19, 2013) (citation omitted).

IV. DISCUSSION

A. The information sought by Plaintiff List is discoverable.

As a threshold matter, List satisfies its burden of establishing that the information sought is relevant under Rule 26. List seeks to prove—through forensic imaging of the hard drive, laptop computer, and desktop computer—that Defendant Umina breached the confidentiality provision of his Employment Agreement and Defendants violated Ohio's Uniform Trade Secret Act.

To prove that Defendant Umina breached the confidentiality provision of his employment agreement, List must demonstrate the existence of a contract, performance, breach of the agreement, and damages. *Brunsman v. W. Hills Country Club*, 151 Ohio App.3d 718, 2003-Ohio-891, 785 N.E.2d 794, ¶ 11 (1st Dist.). List contends that Defendant Umina breached the agreement "by failing to return all of List's property, materials, and proprietary information" as he was required to do under the confidentiality provision of the Employment Agreement. (Doc. #15, *PageID* #98). As to the claim for misappropriation under §1333.61 of the Ohio Trade Secret Act, List must demonstrate "(1) the existence of a trade secret; (2) acquisition of a trade secrete as a result of a confidential relationship; and (3) unauthorized use of a trade secret." *Power Mktg.*

Direct, Inc. v. Ball, No. 2:03-cv-1004, 2004 WL 5826149, *4 (S.D. Ohio April 6, 2004) (quoting *GTI Corp. v. Calhoon*, 309 F. Supp. 762, 767 (S.D. Ohio 1969)).

The information that List seeks is "not information appearing in the text of a document, but rather, the non-visible data contained on a storage device, such as a hard drive." (Doc. #19, *PageID* #260). List contends that forensic imaging is necessary in order to prove both its claims because the images will indicate "whether Umina accessed [] documents after he left List [], whether he copied any of them, whether he used any of their contents to create new, similar documents, or whether he saved, updated, or otherwise manipulated documents, including, specifically, documents containing consumer information." *Id.* at 263.

List specifically argues that forensic imaging is pertinent to the claim for breach of the confidentiality provision because such imaging will demonstrate whether Defendant Umina kept materials on the hard drive after April 11, 2011 in violation of the Employment Agreement. (Doc. #15, *PageID* #98). In addition, List contends that the information sought through forensic imaging is particularly pertinent to the third element of the claim for misappropriation, "unauthorized use," because any manipulation of the files will support the conclusion that Defendant Umina used them to aid Defendant Top Tier. *Id*. In support of both contentions, List points this Court to testimony from Defendant Umina in another proceeding. Defendant Umina testified that "he accessed and used at least one of List's business documents after his termination from List, and while he was employed by [Defendant] Top Tier." *Id.* at 84. In light of Defendant Umina's admission, List "anticipates that an investigation will reveal Umina's

unauthorized access of other materials belonging to List following his termination." *Id.* at 99.

Based on the circumstances, it is reasonable to infer that the hard drive, laptop computer, and desktop computer may contain information central to both of List's claims. This is supported by Defendant Umina's acknowledgement that he accessed and used one of List's documents. (Doc. #15, *PageID* #84). List seeks information about whether Defendant Umina retained confidential company documents and if so, what Defendant Umina may have done with those documents. *Id.* at 87. The forensic imaging, as List convincingly argues, will likely provide the necessary data to answer those key inquiries, and such data cannot be gleaned from mere document review. *Id.* at 94. Rather, List requires access to information, garnered through forensic imaging, that can reveal Defendant Umina's pertinent activity. *Id.* at 94. Thus, although it is yet to be seen whether forensic imaging will in fact yield the exact information that List seeks, List has nevertheless demonstrated that the information it seeks through forensic imaging is discoverable under Rule 26.

B. Plaintiff List is entitled to forensic imaging within certain parameters.

Forensic imaging "is not uncommon in the course of civil discovery." *John B. v. Goetz*, 531 F.3d 448, 459 (6th Cir. 2008) (citing *Balboa Threadworks v. Stucky*, No. 05-1157-JTM-DWB, 2006 WL 763668, at *3 (D. Kan. Mar. 24, 2006)). In fact, federal courts "have assumed that the provisions of Rule 34(a) concerning inspection, copying, and testing of tangible objects are sufficient to authorize a court to order reproduction of an entire hard drive using the 'mirror image' method." *Diepenhorst v. City of Battle*

Creek, No. 1:05-cv-734, 2006 WL 1851243, at *2 (W.D. Mich. June 30, 2006) (citing *Simon Property Group, LP v. MySimon, Inc.*, 194 F.R.D. 639, 640-41 (S.D. Ind. 2000)).

The Sedona Principles, however, urge caution when considering requests for forensic imaging in civil discovery:

> Civil litigation should not be approached as if information systems were crime scenes that justify forensic investigation at every opportunity to identify and preserve every detail. . . . [M]aking forensic image backups of computers is only the first step of an expensive, complex, and difficult process of data analysis that can divert litigation into side issues and satellite disputes involving the interpretation of potentially ambiguous forensic evidence.

The Sedona Principles at 34, 37. Confidentiality and privacy are two reasons for exercising such caution. See Fed. R. Civ. P. 34(a) Advisory Committee Note (2006) ("[c]ourts should guard against undue intrusiveness resulting from inspecting or testing such systems."); *see also FSA US LLC v. Bullock*, No. 17-cv-13972, 2019 WL 258169, at *5 (E.D. Mich. Jan. 18, 2019) (denying forensic imaging request for personal devices containing information about defendant's personal taxes and children's education because, although the information on the devices was important to the plaintiff's claims, the requested imaging was not proportional to the needs of the case).

Courts "have been cautious in requiring the mirror imaging of computers where the request is extremely broad in nature and the connection between the computers and the claims in the lawsuit are unduly vague or unsubstantiated in nature." *John B.*, 531 F.3d at 459-60 (citing *Balboa Threadworks*, 2006 WL 763668, at *3). Thus, mere

suspicion is not enough to justify a forensic imaging request. *See Scotts Co. LLC v. Liberty Mut. Ins. Co.*, No. 2:06-cv-899, 2007 WL 1723509, at *2 (S.D. Ohio June 12, 2007) (denying request found to be an "intrusive examination of its opponent's computer systems on the mere suspicion, based solely on the nature of the claims asserted, that defendant may be withholding discoverable information.").

Moreover, even where forensic imaging has been permitted, the scope of the imaging has not always been without limit. *Ferron v. Search Cactus, L.L.C.*, No. 2:06-cv-327, 2008 WL 1902499 (S.D. Ohio April 28, 2008). The court in *Ferron* provides helpful guidance related to appropriate limitations for forensic imaging. *Id.* In that case, the court attempted to balance the protection of plaintiff's personal confidential information and defendant's concern for deletion of relevant information by ordering a multi-step process. *Id.* First, the plaintiff's expert was directed to mirror image plaintiff's computer hard drives and remove only plaintiff's confidential information. *Id.* at *4. The plaintiff's expert was required to then share the protocol that he used to remove the confidential information with the defendants. *Id.* After this process, the plaintiff had to provide defendant's forensic expert access to the hard drives to complete his own mirror imaging. *Id.* Prior to sharing his findings with the defendant, defendant's forensic expert had to review his findings with plaintiff and give plaintiff an opportunity to identify for deletion any irrelevant or potentially privileged information. *Id.*

Here, Plaintiff List contends that it is entitled to a forensic image of the hard drive as well as forensic images of the laptop and desktop allegedly used to access the contents of the hard drive. Unlike *Scotts*, the request by List is not based on mere suspicion.

Defendant Umina acknowledged in testimony to accessing one of List's business documents after his termination with List and while employed at Defendant Top Tier. (Doc. #15, *PageID* #84). Thus, it is reasonable for List to believe that relevant information may be contained on the hard drive, laptop computer, and desktop computer. Moreover, in contrast to the request in *FSA US LLC*, the request in this case is proportional to the needs of the case. As demonstrated by List, evidence of whether Defendant Umina accessed documents; copied them; saved, updated, or otherwise manipulated them; or used any of their contents to create new, similar documents is necessary to prove its claims against Defendant Umina.

In opposition, Defendants contend that List failed to properly request the forensic imaging of the hard drive and computers during discovery. (Doc. #17, *PageID* #144). Defendants argue that List solely sought to "inspect" the hard drive and any electronic devices that were used to access the information on the hard drive. *Id.* at 144-45. In addition, Defendants posit that the request was satisfied when they (1) agreed to "allow List or its expert to view and physically inspect the electronic devices at a mutually agreeable date, time and place," and (2) "agreed to provide List access to relevant information contained on any of the identified devices, so long as steps were taken to protect irrelevant and personal information from disclosure." *Id.* at 145.

The communications between the parties surrounding this request, however, suggest that Defendants were aware of the scope of List's request and failed to satisfy it—hence the dispute presently pending before the Court. The parties first discussed the need for a forensic image of the hard drive at the parties' Rule 26(f) conference. (Doc.

#19, *PageID* #264). This initial discussion was followed by a series of communication between counsel regarding the forensic imaging and protocol to be used in completing it. *Id*. A formal Request for Inspection of the hard drive and related electronic devices was served on Defendants shortly thereafter. *Id.* This ongoing communication suggests Defendants were well aware of the scope of List's request. Even if the term "inspect" was vague, the representations by List, as well as the discussions about parties' respective forensic imaging experts, make it apparent that List was requesting more than a physical inspection of the devices. Finally, as suggested by List, "[i]f Defendants understood List's requests to be limited in the manner they now argue, [Defendant] Umina would not have objected on the basis that the 'request seeks to inspect or **obtain**…' anything." *Id.* at 265 (emphasis in original).

Defendants additionally present issues of confidentiality and privacy as main concerns in opposition to forensic imaging. According to Defendants, the hard drive contains more than one-million files. (Doc. #17, *PageID* #139). Among those files are many containing Defendant Umina's personal information related to finances (with social security numbers), medical insurance (with identification numbers), personal taxes, personal cell and email communications, and communications to Defendant Umina's attorneys about separate legal matters. *Id*. Additionally, the hard drive contains photographs of Defendant Umina's minor children and familial documents like birth certificates. *Id*. Accepting Defendants' representations of the hard drive as true, some information contained on the hard drive is personal confidential in nature, and thus, like

Ferron, presents valid concerns in favor of limiting discovery. *See also FSA US LLC*, 2019 WL 258169, at *5.

According to List, "[Defendant] Umina's predicament is [] entirely of his own making," because Defendant Umina allegedly co-mingled personal and confidential business information. (Doc. #19, *PageID* #259). In essence, List argues that Defendants' confidentiality and privacy concerns are undermined by the conscious decision Defendant Umina made to retain documents, in violation of the confidentiality provision of the Employment Agreement, and store them with personal documents. *Id*. This argument is not persuasive. Even if Defendant Umina retained documents in violation of his Employment Agreement with List, such conduct does not justify a broad unfettered search of the hard drive containing personal confidential information in order to find evidence to support such a claim. Here, the preservation of confidentiality and privacy for Defendant Umina and his family outweighs the broad access requested by List.

Accordingly, to strike a balance between List's request for discoverable information related to its claims and Defendants' confidentiality and privacy concerns, List's Motion to Compel (Doc. #15) is **GRANTED** pursuant to the following terms:

> 1. Within seven days of the date of this Order, Defendants' forensic computer expert shall create forensic images of the hard drive in Defendant Umina's possession and the laptop and desktop computer Defendant Umina identified as having been used to access the hard drive's contents. Defendants shall preserve these forensic images.
>
> 2. Defendants' forensic computer expert shall then remove only Defendants' confidential personal information from the forensic images of Defendants' hard drive, laptop computer, and desktop computer. Defendants' expert shall provide List

with the protocol he utilized to remove the confidential information.

3. Defendants shall then provide List's computer forensic expert access to the hard drive, laptop computer, and desktop computer.

4. List's forensic computer expert shall produce forensic images of the hard drive, laptop computer, and desktop computer in a reasonable amount of time. List is expected to be considerate with regard to scheduling times that are less intrusive to Defendants.

5. List's expert shall review his findings in confidence with Defendants prior to making any findings available to List.

6. Defendants shall identify for deletion any information that is irrelevant and create a specific privilege log of any relevant information for which they claim privilege. List's computer forensic expert shall remove the information claimed as privileged and provide all other information to List.

7. List's expert shall provide Defendants with the protocol he utilized to remove the privileged information.

IT IS SO ORDERED.

May 1, 2019

s/Sharon L. Ovington
Sharon L. Ovington
United States Magistrate Judge